Alerta de seguridad cibernética	9VSA24-00964-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2024
Última revisión	23 de enero de 2024

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de varios parches informados por varios proveedores para mitigar vulnerabilidades recientemente descubiertas para la interfaz UEFI TianoCore EDKII. Esta última informó que habría al menos 23 proveedores afectados (entre ellos, productos de Lenovo, Intel, AMI, Phoenix, Acer, e Insyde). Nueve de las vulnerabilidades (las primeras nueve listadas a continuación) han sido denominadas en conjunto PixieFAIL.

Vulnerabilidades

CVE-2023-45229	CVE-2023-45232	CVE-2023-45235	CVE-2022-36763
CVE-2023-45230	CVE-2023-45233	CVE-2023-45236	CVE-2022-36764
CVE-2023-45231	CVE-2023-45234	CVE-2023-45237	CVE-2022-36765

Impacto

Vulnerabilidades de riesgo alto:

CVE-2023-45230: El Network Package de EDK2 es susceptible a un desbordamiento de buffer, vulnerabilidad explotable por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de confidencialidad, integridad o disponibilidad. CVSS: 8.8.

CVE-2023-45232: El Network Package de EDK2 es susceptible a una vulnerabilidad de loop infinito, que puede ser explotada por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de disponibilidad. CVSS: 7.5.

CVE-2023-45233: El Network Package de EDK2 es susceptible a una vulnerabilidad de loop infinito, que puede ser explotada por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de disponibilidad. CVSS: 7.5.

CVE-2023-45234: El Network Package de EDK2 es susceptible a un desbordamiento de buffer, vulnerabilidad explotable por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de confidencialidad, integridad o disponibilidad. CVSS: 8.8.

CVE-2023-45235: El Network Package de EDK2 es susceptible a un desbordamiento de buffer, vulnerabilidad explotable por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de confidencialidad, integridad o disponibilidad. CVSS: 8.8.

CVE-2023-45236: El Network Package de EDK2 es susceptible a una vulnerabilidad de TCP Initial Sequence Number predecible, que puede ser explotada por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de disponibilidad. CVSS: 7.5.

CVE-2023-45237: El Network Package de EDK2 es susceptible a una vulnerabilidad de TCP Initial Sequence Number predecible, que puede ser explotada por un atacante para ganar acceso no autorizado y potencialmente llevar a una pérdida de disponibilidad. CVSS: 7.5.

Mitigación

Actualizar a la más reciente versión del firmware UEFI. Disponibles por Tianocore en https://github.com/tianocore/edk2 y por parte de varios proveedores para sus productos, por ejemplo:

Dell: https://www.dell.com/support/kbdoc/es-cl/000215643/dsa-2023-191-security-update-for-tianocore-edk2-vulnerabilities

Microsoft: https://github.com/microsoft/mu_basecore

Lenovo: https://support.lenovo.com/cl/es/solutions/ps500222-tianocore-edk-ii-bios-vulnerabilities

Arm: https://gitlab.arm.com/arm-reference-solutions/edk2

AMI: https://github.com/opencomputeproject/OSF-Aptio-OpenEdition

Phoenix: https://www.phoenix.com/phoenix-securecore/

Algunos productos afectados

Dell: Alienware Area-51m R2, Alienware Aurora R15 AMD, Alienware Aurora R15, Alienware M15 R2, Alienware M15 R3, Alienware m15 R4, Alienware M17 R2, Alienware M17 R3, Alienware m17 R4, Alienware x15 R1, Alienware x17 R1, Dell Embedded Box PC 5000 , Inspiron 5400 AIO, Inspiron 5401 AIO, Inspiron 7700 AIO, Latitude 3180, Latitude 3189, Latitude 3190 2-in-1, Latitude 3190, Latitude 5280/5288, Latitude 5290, Latitude 7200 2-in-1, Latitude 7210 2-in-1, Latitude 7212 Rugged Extreme Tablet, Latitude 7214 Rugged Extreme, Latitude 7280, Latitude 7285 2-in-1, Latitude 7290, Latitude 7300, Latitude 7380, Latitude 7390, Latitude 5400, Latitude 5401, Latitude 5410, Latitude 5411, Latitude 5424 Rugged, Latitude 5480/5488, Latitude 5490, Latitude 5491, Latitude 7400 2-in-1,

Latitude 7400, Latitude 7414 Rugged, Latitude 7424 Rugged Extreme, Latitude 7480, Latitude 7490, Latitude 9410, Latitude 5500, Latitude 5501, Latitude 5510, Latitude 5511, Latitude 5580, Latitude 5591, Latitude 9510, Latitude 5420, Precision 3520, Precision 3530, Precision 3540, Precision 3541, Precision 3550, Precision 3551, Precision 3440 Small Form Factor, Precision 5720 AIO, Vostro 5880, XPS 8960.

Lenovo: 510-15IKL, 510S-08IKL, IdeaCentre 300-20ISH, IdeaCentre 300S-11ISH, ideacentre 310-15IAP, ideacentre 310A-15IAP, ideacentre 310S-08IAP, IdeaCentre 510-15ABR, IdeaCentre 510S-08ISH, IdeaCentre 620s-03IKL, IdeaCentre 700, IdeaCentre 720-18ASR, Legion Y520T_Z370, Legion Y720 Tower, Legion Y720T AMD, Legion Y920 Tower, Lenovo 63, Lenovo H50-30g Desktop, Lenovo M4500, Lenovo M4500 ID, Lenovo M4550 ID, Lenovo V320-15IAP, QITIAN 4500, QITIAN 4500-C, QITIAN B2300, QITIAN B4550, QITIAN B4650, QITIAN B5900, QITIAN M2300, QITIAN M4550, QITIAN M4600, QITIAN M4650, QT M410/B415/M415, ThinkCentre E73 (SFF), ThinkCentre E73 (TWR), ThinkCentre E73s, ThinkCentre E74, ThinkCentre E74s, ThinkCentre E75 t/s, ThinkCentre E93 (SFF), ThinkCentre E93 (TWR), ThinkCentre M4500k, ThinkCentre M4500q, ThinkCentre M4500t/s, ThinkCentre M4600t/s, ThinkCentre M600, ThinkCentre M610, ThinkCentre M625q, ThinkCentre M6500t/s, ThinkCentre M6600, ThinkCentre M6600q, ThinkCentre M6600t/s, ThinkCentre M700q, ThinkCentre M700t/s, ThinkCentre M710e, ThinkCentre M710q, ThinkCentre M710t/s, ThinkCentre M715q, ThinkCentre M715t/s, ThinkCentre M73 (SFF), ThinkCentre M73 (TWR), ThinkCentre M73 Tiny, ThinkCentre M73p, ThinkCentre M79 (SFF), ThinkCentre M79 (TWR), ThinkCentre M800, ThinkCentre M83 (SFF), ThinkCentre M83 (Tiny), ThinkCentre M83 (TWR), ThinkCentre M8500t/s, ThinkCentre M8600t/s, ThinkCentre M900, ThinkCentre M910 t/s, ThinkCentre M910q, ThinkCentre M910x, ThinkCentre M93, ThinkCentre M93P (SFF), ThinkCentre M93P (TWR), ThinkCentre M93P Tiny, ThinkCentre S510, V520s-08IKL, V520t-15IKL, YANGTIAN AfH110, YANGTIAN AfH81, YANGTIAN AfQ150, YANGTIAN Mc H110, YANGTIAN Mc H110 PCI, YANGTIAN Mc H81, YANGTIAN Me/We H110, YANGTIAN Mf/Wf H110 PCI, YANGTIAN Mf/Wf H81 PCI, YANGTIAN Ms/Ws H81, YANGTIAN Tc/Wc H110 PCI, YANGTIAN TC/WCc H81 PCI, YANGTIAN YTM6900e-00, YTA8900f, Desktop - All in One, AIO300-23ISU(C5130), AIO310-20IAP, AIO520-22IKL, AIO520-22IKU, AIO520-24IKL, AIO520-24IKU, AIO520-27IKL, AIO720-24IKB, AIO910-27ISH, IdeaCentre 520S-23IKU, IdeaCentre 730S-24IKB, Lenovo S200z(S2010), QITIAN A3300, QT A7400, QT A8150, ThinkCenter M700z, ThinkCenter M800z, ThinkCentre E73Z (AIO), ThinkCentre E74z, ThinkCentre E93Z (AIO), ThinkCentre E95z, ThinkCentre M700z, ThinkCentre M7200z, ThinkCentre M7250z, ThinkCentre M7300z, ThinkCentre M73Z (AIO), ThinkCentre M800z, ThinkCentre M810z, ThinkCentre M818z, ThinkCentre M8200z, ThinkCentre M8250z, ThinkCentre M8300z, ThinkCentre M8350z, ThinkCentre M83Z (AIO), ThinkCentre M900Z, ThinkCentre M910z, ThinkCentre M9500z, ThinkCentre M9550z, ThinkCentre X1 AIO, V310z(YT S3150), V410z(YT S4250), V510z (YT S5250), YANGTIAN S3040, YANGTIAN S800, IdeaPad, 120s-11IAP, 120s-14IAP, 130-14IKB, 130-15AST, 130-15IKB, 300e, 310S-11IAP, 320-17ABR, 320-17AST, 320C-15IKB, 320S-13IKB, 320S-14IKB, 320S-15IKB, 320S-15ISK, 330-14AST, 330-14IGM, 330-14IKB, 330-14IKBR, 330-15ARR, 330-15ARR Touch, 330-15AST, 330-15ICH, 330-15IGM, 330-15IKB, 330-15IKBR, 330-15IKBR Touch, 330-17AST, 330-17ICH, 330-17IKB, 330-17IKBR, 330C-14IKB, 330C-15IKB, 330S-14AST, 330S-15ARR, 330S-15AST, 330S-15IKB GTX1050, 520-15IKBR, 520S-14IKB, 530s-14ARR, 530S-14IKB, 530S-15IKB, 720S Touch-15IKB, 720S-13ARR, 720S-13IKBR, 720S-14IKB, 720S-14IKBR, 720S-15IKB, D330-10IGM, D335-10IGM, E42-80, E4-ARR, E52-80, Flex 4-1130, FLEX 5-1570(R), FLEX 6-11IGM, FLEX 6-14ARR, FLEX 6-14IKB, K21-80, K22-80, K32-80, K41-80, K42-80, K42-80 ISK, K43c-80,

Legion Y530-15ICH, Legion Y530-15ICH(1060), Legion Y730-15ICH, Legion Y730-15ICHg, Legion Y730-17ICH, Legion Y730-17ICHg, Legion Y9000K 2019, Lenovo E41-20, Lenovo E41-25(CZ-L), Lenovo ideapad 320-14AST, Lenovo ideapad 320-15ABR, Lenovo ideapad 320-15AST, Lenovo V720-14, Lenovo XiaoXin 14AST/XX CHAO7000-14AST, Lenovo XiaoXin 15AST/XX CHAO7000-15AST, Lenovo Y520-15IKBM, MIIX 520-12IKB, MIIX 525-12IKB, MIIX 720-12IKB, N22P（Lenovo 100e）, N24, RESCUER Y7000, RESCUER Y7000P, RESCUER Y7000P(1060), RESCUERY7000(1060), S530-13IWL, V110-14AST, V110-14IAP, V110-14IKB, V110-15AST, V110-15IAP, V110-15IKB, V110-15ISK, V110-17IKB, V110-17ISK, V130-14IGM, V130-14IKB, V130-15AST, V130-15IGM, V130-15IKB, V145-14AST, V145-15AST, V310-14IKB, V310-14ISK, V310-15IGM, V310-15IKB, V310-15ISK, V320-14IKB, V320-15IKB, V320-17IKB, V320-17IKBR, V320-17ISK, V330-14AAR, V330-14AST, V330-14IGM, V330-14IKB, V330-14ISK, V330-15AST, V330-15IGM, V330-15IKB, V330-15ISK, V510-14IKB, V510-15IKB, V720-12, V730-13IKB, V730-13ISK, V730-15IKB, WEI5-14IKB, WEI5-15IKB, XiaoXin 15ARR/XX CHAO7000-15ARR, XiaoXin Air 14ARR, XiaoXin Air 14IKBR, XiaoXin Air 15IKBR, XXCHAO7000-15IKBRN, Yoga 310-11IAP, YOGA 330-11IGM, YOGA 520-14IKBR, YOGA 530-14ARR, YOGA 530-14IKB, YOGA 720-12IKB, Yoga 730-15IKB, YOGA 920-13IKB/YOGA 920-13IKB Glass, YOGA C930-13IKB/YOGA C930 Glass, YOGA730-13 IKB, Yoga730-13IWL, Yoga730-15IWL, **小新 潮**7000-13, **小新 潮**7000-15 U22, **小新 潮**7000-15 U42, **昭阳**E43-80, **昭阳**E53-80, Storage, B300 Fiber Channel Switch, B6505 Fiber Channel Switch, B6510 Fiber Channel Switch, D1212/D1224 Series Expansion, D3284 HD JBOD/EBOD, E1212/E1224 EXP2, Lenovo Storage D1012/D1024, Lenovo Storage E1012/E1024 (WW), Lenovo Storage SBOD (PRC), Lenovo V3700 V2, Lenovo V3700 V2 XP, Lenovo V5030/V5030F, Lenovo V7000 (PRC), N3310 (Adapted from RD350), N4610 (Adapted from RD650), S2200/3200 (PRC), S2200/S3200 (WW), StorSelect DX8200C (x3650 M5), StorSelect DX8200D (x3650 M5), StorSelect DX8200N (x3650 M5), ThinkPad, ThinkPad 10, ThinkPad 11e / ThinkPad 11e Yoga, ThinkPad 11e 3rd Gen/Yoga 11e, ThinkPad 11e 4th Gen / ThinkPad 11e Yoga, ThinkPad 11e/Yoga 11e, ThinkPad 11e/Yoga 11e(Braswell), ThinkPad 13 2nd Gen/ThinkPad S2 2nd Gen, ThinkPad 13/ ThinkPad S2, ThinkPad A275, ThinkPad A475, ThinkPad E450/E450c/E550/E550c, ThinkPad E455/E555, ThinkPad E460/E560, ThinkPad E465/E565, ThinkPad E470/E570, ThinkPad E475/E575, ThinkPad E480/E580, ThinkPad E485/E585, ThinkPad E570p / ThinkPad S5, ThinkPad Edge E445/E545, ThinkPad Helix, ThinkPad L380 / S3 3rd Gen, ThinkPad L380 Yoga / S2 Yoga 3rd Gen, ThinkPad L430/L530, ThinkPad L440/L540, ThinkPad L450, ThinkPad L460, ThinkPad L470, ThinkPad L480/L580, ThinkPad L560, ThinkPad L570, ThinkPad P1, ThinkPad P40 Yoga, ThinkPad P50, ThinkPad P50s, ThinkPad P51, ThinkPad P51s, ThinkPad P52, ThinkPad P52s, ThinkPad P70, ThinkPad P71, ThinkPad P72, ThinkPad S1 Yoga (Non-vPro), ThinkPad S1 Yoga (vPro), ThinkPad S1 Yoga 12, ThinkPad S3 Yoga 14, ThinkPad S430, ThinkPad S5 Yoga 15, ThinkPad S5/E560p, ThinkPad S531, ThinkPad S540, ThinkPad T25, ThinkPad T430, T430i, ThinkPad T430s, ThinkPad T431s, ThinkPad T440/T440s, ThinkPad T440p, ThinkPad T450/T450s, ThinkPad T460, ThinkPad T460p, ThinkPad T460s, ThinkPad T470, ThinkPad T470p, ThinkPad T470s, ThinkPad T480, ThinkPad T480s, ThinkPad T530, T530i, ThinkPad T540/T540p, ThinkPad T550, ThinkPad T560, ThinkPad T570, ThinkPad T580, ThinkPad Tablet 10 (32-bit), ThinkPad Tablet 10 (64-bit), ThinkPad Tablet 8 (32-bit), ThinkPad Tablet 8 (64-bit), ThinkPad Twist/S230u, ThinkPad W530, ThinkPad W540/W541, ThinkPad W550s, ThinkPad X1 Carbon, ThinkPad X1 Carbon, X1 Yoga, ThinkPad X1 Extreme, ThinkPad X1 Tablet, ThinkPad X1 Yoga, ThinkPad X131e (AMD), ThinkPad X131e (Intel), ThinkPad X140e (AMD), ThinkPad X230 Tablet; X230i Tablet, ThinkPad X230, X230i, ThinkPad X230s/X231s, ThinkPad X240, ThinkPad X240s, ThinkPad X250, ThinkPad X260, ThinkPad X270,

ThinkPad X280, ThinkPad X380 Yoga, ThinkPad Yoga 11e, ThinkPad Yoga 11e 5th Gen, ThinkPad 11e 5th Gen, ThinkPad 11e 6th Gen, ThinkPad Yoga 14 460 S3, ThinkPad Yoga 260, S1, ThinkPad Yoga 370 /ThinkPad S1 3rd, ThinkServer, ThinkServer RD350G, ThinkServer RD340, ThinkServer RD350, ThinkServer RD440, ThinkServer RD450, ThinkServer RD550, ThinkServer RD640, ThinkServer RD650, ThinkServer RQ750, ThinkServer RS140, ThinkServer RS160, ThinkServer TD340, ThinkServer TD350, ThinkServer TS140, ThinkServer TS150, ThinkServer TS240, ThinkStation, ThinkStation C30 (1136-1137), ThinkStation D30 (4353-4354), ThinkStation E32, ThinkStation P300, ThinkStation P310, ThinkStation P318, ThinkStation P320, ThinkStation P320 Tiny, ThinkStation P410, ThinkStation P500, ThinkStation P510, ThinkStation P520, ThinkStation P520c, ThinkStation P700, ThinkStation P710, ThinkStation P720, ThinkStation P900, ThinkStation P910, ThinkStation P920, ThinkStation S30 (4351-4352), ThinkSystem, Product , ThinkSystem HR630X, ThinkSystem HR650X , ThinkSystem ODC5200-CN350M , ThinkSystem ODC5200-CN650S, ThinkSystem SD350, ThinkSystem SD530, ThinkSystem SD650, ThinkSystem SN550, ThinkSystem SN850, ThinkSystem SR150, ThinkSystem SR250, ThinkSystem SR530, ThinkSystem SR550, ThinkSystem SR570, ThinkSystem SR590, ThinkSystem SR630, ThinkSystem SR650, ThinkSystem SR850, ThinkSystem SR860, ThinkSystem SR950, ThinkSystem ST250, ThinkSystem ST50, ThinkSystem ST550, ThinkSystem ST558,.

Otros enlaces
https://uefi.org/
}https://github.com/tianocore/edk2
https://www.kb.cert.org/vuls/id/132380
https://blog.quarkslab.com/for-science-using-an-unimpressive-bug-in-edk-ii-to-do-some-fun-exploitation.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.24 17:04:14 -03'00'